

**Notice of Allowability**

Application No.

10/025,541

Examiner

Brandon S. Bludau

Applicant(s)

MOORE ET AL.

Art Unit

2132

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 3/20/2006.
2. ☒ The allowed claim(s) is/are 1,4,5,7-11,14,15,17-21,24,25 and 27-38.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                    |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material          | 8. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance              |
|   | 9. <input type="checkbox"/> Other _____.   |

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin Zilka on 04/06/2006 and email correspondence on 04/10/2006. The application has been amended as follows:

#### IN THE CLAIMS

Amend the claims as follows:

1. (Currently Amended) A computer program product embodied on a computer readable medium operable for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:
    - searching code operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;
    - context identifying code operable to identify a context within said computer file of said one or more target words; and
    - file identifying code operable ~~if said context matches one or a predetermined set of contexts~~ to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;
- wherein said predetermined word library includes one or more of:
- words that are names associated with known malware authors;
  - word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;  
wherein said predetermined set of contexts includes one or more of:  
within a script portion of a webpage;  
within a comment of a webpage; and  
within a predetermined proximity to another target word;

wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

4. (Currently Amended) A computer program product as claimed in claim 1, wherein, ~~if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found actions~~ as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

14. (Currently Amended) A method as claimed in claim 11, wherein, ~~if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found actions~~ as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

21. (Currently Amended) Apparatus including a program embodied on a computer readable medium for identifying a computer file as potentially containing malware, said apparatus comprising:

searching logic operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying logic operable to identify a context within said computer file of said one or more target words; and

Art Unit: 2132

file identifying logic ~~operable if said context matches one or a predetermined set of contexts~~ to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

24. (Currently Amended) Apparatus as claimed in claim 21, wherein, ~~if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found actions~~ as a result of the one or more other malware identifying processes, identified malware is acted upon with one or more malware found actions.

36. (Currently Amended) A computer program product embodied on a computer readable medium ~~operable~~ for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code ~~operable~~ to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

Art Unit: 2132

context identifying code operable to identify a context within said computer file of said one or more target words; and

file identifying code ~~operable if said context matches one or a predetermined set of contexts~~ to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage; and

within a predetermined proximity to another target word;

wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

38. (Currently Amended) Apparatus including a program embodied on a computer readable medium for identifying a computer file as potentially containing malware, said apparatus comprising:

searching logic operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying logic operable to identify a context within said computer file of said one or more target words; and

file identifying logic ~~operable if said context matches one or a predetermined set of contexts~~ to identify said computer file as potentially containing malware, if said context matches one or a predetermined set of contexts;

Art Unit: 2132

wherein said predetermined word library includes one or more of:

- words that are names associated with known malware authors;
- word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and
- word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author;

wherein said predetermined set of contexts includes one or more of:

- within a script portion of a webpage;
- within a comment of a webpage; and
- within a predetermined proximity to another target word;

wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

### **Reasons for Allowance**

The following is an examiner's statement of reasons for allowance: The independent claims are deemed allowable due to the subsequent inclusion of the allowable subject matter previously in dependent form as stated in the previous action.

This amendment is necessitated by a 112 problem that occurred as a result of the inclusion of the allowable matter into the independent claims. The affected dependent claims have been amended in this action to overcome the resultant 112 issues.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

Art Unit: 2132

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

**Conclusion**


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau  
Examiner  
Art Unit 2132

BB  
\*\*\*

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100